Information Security Managers Group
Thursday, January 27, 2011 Meeting Minutes

MEETING LOGISTICS (all meeting minutes are posted on the [ISMG Sharepoint](#) site)

When: Last Thursday of each month 1:00 pm – 2:30 pm
Who: Agency CIO and/or Information Security Manager
Where: Department of Labor and Industry 3rd Floor Conference Room,
                 Walt Sullivan Building, Corner of Lockey and Sanders
Next Meeting: Tentative – February 24, 2011 1:00 pm

PRESENT

DEQ: Michael Jares
DOA: Kevin Winegardner – Chair
MDT: Kristi Antosh
HHS: Jackie Thiel
MPERA: Dave Swenson
DLI: Judy Kelly
DLI: Lance Wetzel
DNR: Rick Bush

Guests: Michael Sweeney- DOA IT Mgr
               Larry Manchester – State CIO Policy Office

PURPOSE

The Information Security Managers Group has three primary purposes:
- Advise the State CIO on Information Risk Management Issues at the Statewide level
- Raise awareness while identifying communities of interest for EPP purposes
- Provide a forum for agency exchange of information

AGENDA ITEMS

- **Welcome and (re)introductions**
  - Mr. Dave Swenson was introduced and all members then introduced themselves to Mr. Swenson.

- **Training on NIST Controls – Control Family – Program Management Control PM-5– "Information System Inventory".**
  - Deferred at Chairs request due to agenda priorities.

- **Status Update**: The State CIO has required some additional re-work regarding the ISMG recommendation to rescind the legacy IT security policies [Internet and Intranet Security](#) and [Internet Filtering](#). Appropriate procedures are necessary prior to rescinding the legacy policies. Group decided to add additional language to decision brief to address reason for rescission decision and impacts of decision.
  - **Action**:
    - Brief returned to CIO Policy Office for rework. CIO Policy Office has the action for required products. Draft products to be posted under ISMG Projects in the Legacy Policies Review Project under the [Internet Filtering](#)

- and Intranet Security folder. Deadline for review to be assigned when posted.

- **Status Update:** "Statewide Standard: Access Control" and "Statewide Standard: Identification and Authentication"
  - Standard content (language), under review by State CIO and executive staff. After approval next step in process is DOA Legal review.

- **Discussion:** Group continued discussion on tasking from State CIO to produce a charter for a Statewide Information Risk Management Program. Group decided to reword instrument to be more concise, focusing on intent, who does what, etc. Charter should be current at the beginning and for the lifecycle of the program. Chair will revise document and repost for editing by the ISMG membership.
    - **Action**:
      - ISMG members to continue review of sample charter document and recommend edits. Continue conversation online and place on agenda for February. Note: finished draft of charter will be delivered to State CIO by March 1st, 2011. Sample charter document is here under Draft SIRMP Charter folder.
        - **Who**: Chair and ISMG

- **Discussion**: Next legacy policy for ISMG review; "User Responsibilities" and related legacy policies, "Computer Virus Detection and Protection" and "Transmission Privacy". Others?

OTHER PENDING ACTION ITEMS (Continued)

- Develop a visual representation of Policy, Standard of Performance, Guideline, and Procedure taxonomy. Post to ISMG Sharepoint site. (Companion Visual to go with spreadsheet "Connect Dots Ext Req to Procedures"
  - ISMG Chair

- Revise ISMG Sharepoint site to be more of a visual representation of a NIST based Program.
  - ISMG Chair

AGENDA ITEMS FOR NEXT MEETING

- **Training** on NIST Controls – Control Family – Program Management Control PM-5– "Information System Inventory"
  - ISMG Chair
- **Legacy Policies Status Update**: Status of decision package recommendation for State CIO regarding the legacy IT security policies Internet and Intranet Security and Internet Filtering
  - Chair
- **Discuss on next legacy IT policies to review**: "User Responsibilities" and related legacy policies, "Computer Virus Detection and Protection" and "Transmission Privacy". Others?
  - Development Team (ISMG)
- **Report** out on In-House NIST Training opportunity with MISTI
  - MDT ISM